

ABSTRACT

A method for processing communication traffic includes monitoring the communication traffic that is directed to a group of addresses on a network, and determining respective baseline characteristics of the communication traffic that is directed to each of the addresses in the group. Deviations from the respective baseline characteristics of the communication traffic directed to at least one of the addresses in the group are detected, as an indication that at least some of the communication traffic may be of malicious origin. Responsively to detecting the deviation, the communication traffic that is directed to all of the addresses in the group is filtered so as to remove at least some of the communication traffic that is of the malicious origin.